Active response

Remove file & folder

Visual Studio Code

- allowed_items > Fichiers/Dossiers déjà présents
- Lors du scan, si le nom n'apparaît pas dans la liste blanche, alors il sera supprimé.

```
import os
import shutil

# Dossier à surveiller
folder_path = r"C:\Users\Public\Wazuh_active-response"

# Liste blanche des fichiers et dossiers autorisés
allowed_items = {
    "keepme.txt",
    "config.ini",
    "safe-folder"
}

for item in os.listdir(folder_path):
    item_path = os.path.join(folder_path, item)

    if item not in allowed_items:
        try:
            if os.path.isfile(item_path):
                os.remove(item_path)
                print(f"**WAZUH-AR** Fichier supprimé : {item_path}")
            elif os.path.isdir(item_path):
                shutil.rmtree(item_path)
                print(f"**WAZUH-AR** Dossier supprimé : {item_path}")
        except Exception as e:
```

```
            print(f"**WAZUH-AR** Erreur lors de la suppression de {item_path} :
{str(e)}")
```

exécutable

Le rendre exécutable >> pyinstaller -F @name

emplacement script

C:\Program Files (x86)\ossec-agent\active-response\bin

ossec.conf

```
<command>
  <name>remove-file.py</name>
  <executable>clean_new_files.exe</executable>
  <timeout_allowed>yes</timeout_allowed>
</command>
```

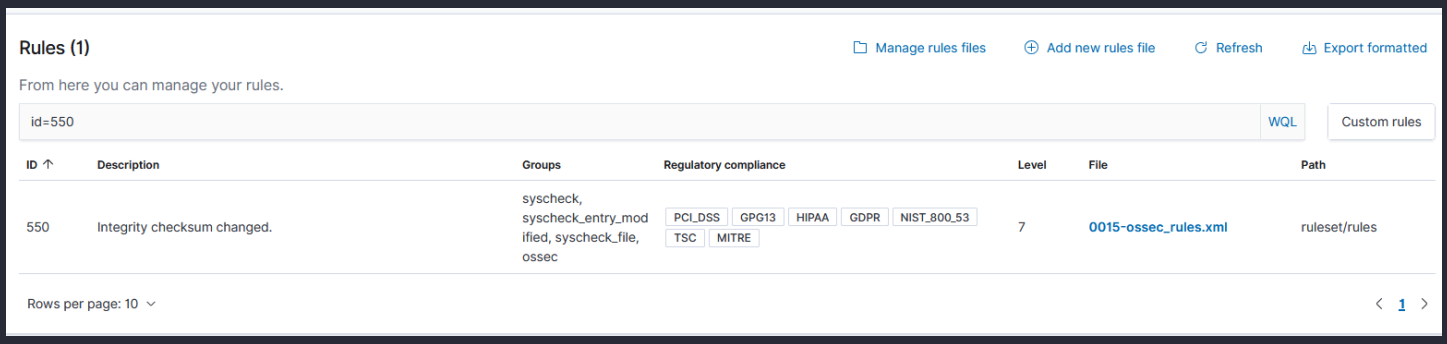
active-response conf

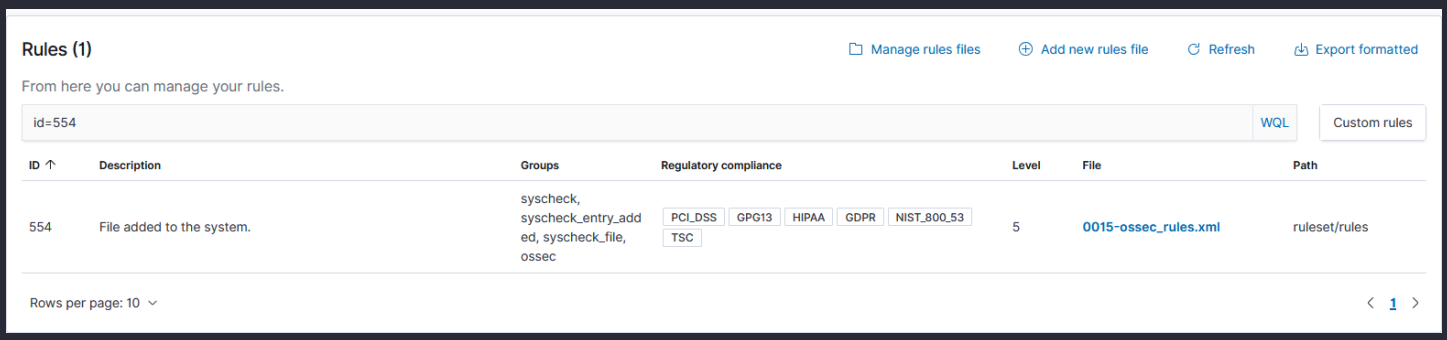
Toujours dans le ossec.conf

```
<active-response>
  <command>clean-new-files</command>
  <location>local</location>
  <rules_id>100001</rules_id>
</active-response>
```

- rules id >> Si la règle est déclenchée, alors ca va activer le script, à adapter selon les besoins

Pour ma part, ce sera les règles '550, 554'





```
<command>
  <name>remove-file.py</name>
  <executable>clean_new_files.exe</executable>
  <timeout_allowed>yes</timeout_allowed>
</command>

<!-- Active response -->

<active-response>
  <command>clean-new-files</command>
  <location>local</location>
  <rules_id>550,554</rules_id>
</active-response>
```

syscheck

Il faut que le module 'FIM' surveille le dossier pour détecter la règle 'syscheck' :

```
<agent_config os="Windows">
  <syscheck>
    <directories check_all="yes" report_changes="yes" realtime="yes">C:\Users\*\Documents</directories>
    <directories check_all="yes" report_changes="yes" realtime="yes">C:\Users\Public</directories>
  </syscheck>
</agent_config>
```

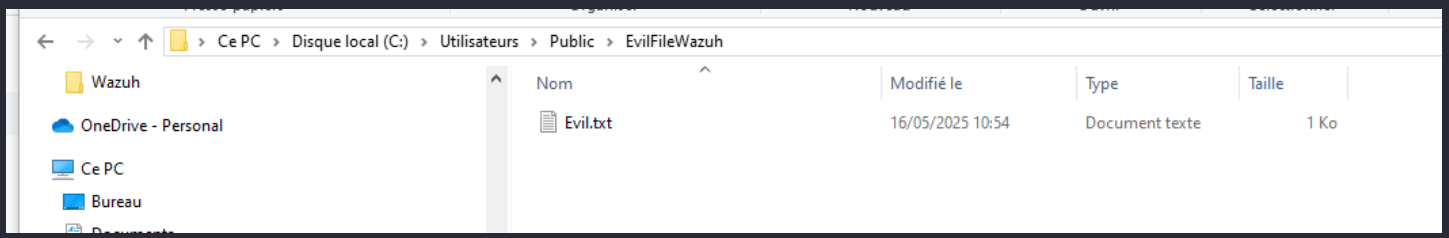
powershell agent

- Restart-Service -Name WazuhSvc
- Get-Service -Name WazuhSvc

wazuh server

- systemctl restart wazuh

Vérifications



May 16, 2025 @ 10:54:33.171 syscheck.mode: realtime syscheck.path: c:\users\public\evilfilewazuh\nouveau document texte.txt syscheck.sha1_after: da39a3ee5e6b4b0d3255bfef95601890afd80709 syscheck.uname_after: rchar syscheck.mtime_after: May 16, 2025 @ 12:54:30.000 syscheck.attrs_after: ARCHIVE syscheck.size_after: 0 syscheck.uid_after: S-1-5-21-299502267-1482476501-725345543-13652 syscheck.win_perm_after.allowed: DELETE, READ_CONTROL, WRITE_DAC, WRITE_OWNER, SYNCHRONIZE, READ_DATA, WRITE_DATA, APPEND_DATA, READ_EA, WRITE_EA, EXECUTE, READ_ATTRIBUTES, WRITE_ATTRIBUTES, DELETE, READ_CONTROL, WRITE_DAC, WRITE_OWNER, SYNCHRONIZE, READ_DATA, WRITE_DATA, APPEND_DATA, READ_EA, WRITE_EA, EXECUTE, READ_ATTRIBUTES, WRITE_ATTRIBUTES, DELETE, READ_CONTROL, WRITE_DAC, WRITE_OWNER, SY

May 16, 2025 @ 10:54:10.219 syscheck.mode: realtime syscheck.path: c:\users\public\alertwazuhmaybe\alertforwazuhtest.txt syscheck.sha1_after: d1e1baacc2e051112c84ffead79e65ca640235b8 syscheck.uname_after: rchar syscheck.mtime_after: May 16, 2025 @ 12:44:07.000 syscheck.attrs_after: ARCHIVE syscheck.size_after: 186 syscheck.uid_after: S-1-5-21-299502267-1482476501-725345543-13652 syscheck.win_perm_after.allowed: DELETE, READ_CONTROL, WRITE_DAC, WRITE_OWNER, SYNCHRONIZE, READ_DATA, WRITE_DATA, APPEND_DATA, READ_EA, WRITE_EA, EXECUTE, READ_ATTRIBUTES, WRITE_ATTRIBUTES, DELETE, READ_CONTROL, WRITE_DAC, WRITE_OWNER, SYNCHRONIZE, READ_DATA, WRITE_DATA, APPEND_DATA, READ_EA, WRITE_EA, EXECUTE, READ_ATTRIBUTES, WRITE_ATTRIBUTES, DELETE, READ_CONTROL, WRITE_DAC, WRITE_OWNER, SY

	Time	rule.description	rule.id	rule.level	agent.name	data.url
>	May 16, 2025 @ 10:55:44.790	Integrity checksum changed.	550	7	INFO027W10	-
>	May 16, 2025 @ 10:55:43.766	Integrity checksum changed.	550	7	INFO027W10	-
>	May 16, 2025 @ 10:55:42.499	Integrity checksum changed.	550	7	INFO027W10	-